

REMARKS

The following remarks are prepared in response to the final Office Action of September 26, 2005. Claims 1-34 are pending in this application, after entry of this amendment. Applicant respectfully traverses and requests reexamination.

Rejection Under 35 U.S.C. § 112, ¶ 2

Claims 1, 12, 15, 17 and 22-34 were rejected under 35 U.S.C. § 112, ¶ 2 as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Applicant has amended claims 1, 12, 15, 17 and 22-34 to more clearly define the invention. Applicant respectfully requests that the rejection of claims 1, 12, 15, 17 and 22-34 under 35 U.S.C. § 112, ¶ 2 be withdrawn.

Rejection Under 35 U.S.C. § 103(a)

Claims 1-3, 11-12, 15, 17-19, 21-29 and 31-34 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hirose (U.S. Patent No. 5,917,915, hereinafter Hirose) in view of Akiyama (U.S. Patent No. 6,463,155, hereinafter Akiyama).

The Hirose Patent

Hirose's invention has been conceived in view of the following problem. If the newspaper data (namely, scrambled newspaper data) have been received prior to the establishment of a contract are recorded on the recording medium, after the establishment of the contract, even if the contractor may have his own scramble key, he cannot decrypt the scrambled newspaper data which have been recorded on this recording medium (see Hirose, column 2, lines 8-14).

Hirose discloses a scramble apparatus comprising an entire scramble means (e.g., data scrambler 14 shown in FIG. 3) for scrambling an entire portion of the data, and block unit scramble means (e.g., information unit scramble processing unit 27 shown in FIG. 2) for selectively scrambling the data in a preselected block unit (see Hirose, column 3, lines 16-21).

Hirose discloses a descramble apparatus comprising an entire descramble means (e.g., data scrambler 87 shown in FIG. 5) for descrambling the entire portion of data scrambled by the entire scramble means, and block unit descramble means (e.g., information unit scramble processing unit 31 of FIG. 6) for descrambling the data scrambled in a predetermined block unit by the block unit scramble means (see Hirose, column 3, lines 28-35). In this descramble apparatus, when this apparatus further includes storage means (e.g., recording medium 8 shown in FIG. 6) for storing the data descrambled by the entire descramble means, the data stored in the storage means is descrambled by the block unit descramble means (see Hirose, column 3, lines 36-40). When this apparatus further includes read means (e.g., IC card interface apparatus 111 shown in FIG. 11) for reading a scramble key from the storage medium for storing the scramble key used to descramble the data scrambled in the predetermined block unit by the block unit scramble means, the data can be descrambled by the block unit descramble means with employment of the scramble key read from the read means (see Hirose, column 3, lines 40-47).

The Akiyama Patent

Akiyama's invention has been conceived in view of the following problem. Akiyama's invention has an object of formulating a broadcast reception device capable of realizing conditional access while maintaining the safety level even when the broadcast bandwidth is narrow or when the number of contractors has increased beyond the expectation.

In Akiyama, a unique master key is provided for each broadcast reception device separately, and a broadcast transmission device scrambles broadcast contents using a work key which is a key uniquely defined for each channel, and encrypts, before transmission, the work key using a master key unique to a broadcast reception device under contract, thereby realizing conditional access. In addition, the work key is set up for each contract period (usually one month).

Akiyama prepares a master key that is commonly provided with respect to all broadcast reception devices, and reception device IDs that correspond to the broadcast reception devices respectively. A broadcast transmission device encrypts contract information together with a corresponding reception device ID using the master key and then transmits them. The broadcast transmission device also scrambles the broadcast contents using a channel key and transmits it. The channel key is transmitted either in the encrypted form or as is. In the case of encrypting the channel key, a corresponding channel-key decryption key is also transmitted. Meanwhile, the broadcast reception device retains the master key and a reception device ID in advance. The retained master key is used to decrypt the contract information and the received reception device ID, while the contract information is identified according to judgment of whether the retained reception device ID matches the decrypted reception device ID. The identified contract information facilitates efficient conditional access. Akiyama states that this structure enables a user to reproduce contents of a contracted channel, exclusively within the contract period.

The Present Invention

The present invention has been conceived in view of the following problem. In the storage service, when reproducing scrambled content in storage, it difficult to realize a sufficient

performance level of the particular reproduction modes, such as fast-forward speed (see Description of the Prior Art).

The reception apparatus receives and stores storage information in which a list of descrambling keys including all descrambling keys to be used for descrambling the scrambled content and descrambling key identifiers that identify the descrambling keys respectively and are used to identify a descrambling key corresponding to the predetermined unit of scrambled content in both a normal reproduction mode and a particular reproduction mode is embedded and scrambled content. Thereafter, the reception apparatus extracts from the stored scrambled content a predetermined unit of the scrambled content either sequentially if in the normal reproduction mode or in an order different from the normal reproduction mode if in the particular reproduction mode.

Furthermore, the reception apparatus specifies and extracts a descrambling key corresponding to the predetermined unit of scrambled content from the extracted list of scrambling keys using the descrambling key identifiers in both the normal reproduction mode and the particular reproduction mode, and descrambles the extracted predetermined unit of scrambled content using the extracted descrambling key. The reception apparatus further reproduces the predetermined unit of descrambled content in both the normal reproduction mode and the particular reproduction mode.

Independent Claims 1, 12, 15, 17 and 22-34

Claims 1, 12, 15, 17 and 22-34 have been amended to recite “descrambling key identifiers that identify the descrambling keys respectively and are used to identify a descrambling key corresponding to the predetermined unit of scrambled content in both a normal reproduction mode and a particular reproduction mode.” That is, a special reproduction mode

can be pursued in the same procedure as a normal reproduction mode. Also, claims 1, 12, 22, 23, 26, 27, 31 and 32 have been amended to recite “specifying and extracting a descrambling key corresponding to the predetermined unit of scrambled content from the extracted list of descrambling keys using the descrambling key identifiers in both the normal reproduction mode and the particular reproduction mode.”

The extraction of the descrambling key can be executed in a short time and at low load, which improves the performance of particular reproduction processes, such as fast forward speed, to a sufficient level (see Summary of the Invention). The performance level of the particular reproduction modes (especially fast-forward speed) of the scrambled content in storage is improved. The claims have been amended to identify a necessary descrambling key swiftly even when the descrambling keys are required in an extraordinary order. So as to realize this, the descrambling keys are stored as a list together with specification information. According to this construction, the present invention can extract a necessary descrambling key swiftly using the specification information, even when a special reproduction mode is selected for reproducing content in the storage. As a result, the content reproduction is performed smoothly.

The key specifying information for specifying a descrambling key corresponds to a list of descrambling keys including all descrambling keys to be used for descrambling the scrambled content and descrambling key identifiers that identify the descrambling keys respectively and are used to identify a descrambling key corresponding to the predetermined unit of scrambled content in both a normal reproduction mode and a particular reproduction mode. The list of descrambling keys is a list including all the descrambling keys and is for facilitating search of a desired descrambling key. By searching for a desired descrambling key from this list, it becomes possible to improve the performance of particular reproduction processes to a fully satisfactorily

level as well as directly contributing to the improvement of security level because the list includes the descrambling keys.

On page 10 of the final Office Action, the Examiner acknowledges that Hirose does not explicitly disclose key specifying information for specifying a descrambling key. Applicant asserts that Akiyama does not remedy the deficiency of Hirose. That is, Akiyama does not teach or suggest key specifying information for specifying a descrambling key. Therefore, it follows that Akiyama does not teach or suggest descrambling key identifiers that identify the descrambling keys respectively and are used to identify a descrambling key corresponding to the predetermined unit of scrambled content in both a normal reproduction mode and a particular reproduction mode.

Akiyama discloses reception contract information containing contract information and a corresponding reception device ID. The reception contract information is not the same as the key specifying information. The reception contract information of Akiyama does not contain any key information but rather is used to transmit to each broadcast transmission device corresponding contract contents, from the broadcast transmission device. Hence, the reception contract information inherently does not contribute to improvement of the performance of particular reproduction processes. In addition, because the reception contract information inherently does not contain any descrambling key, it cannot directly contribute to improvement of security level.

Furthermore, Akiyama discloses that the work key is set up for each contract period (usually one month). Hence, Akiyama assumes that only one common descrambling key (i.e., a work key) is used with the plurality of broadcast reception devices. Akiyama does not contemplate a system equipped with high security so that a plurality of descrambling keys

alternate with each other in a short period of time. Accordingly, Akiyama fails to disclose the list of descrambling keys. For at least the reasons discussed above, Applicant submits that claims 1, 12, 15, 17 and 22-34 are patentably distinct over Hirose in view of Akiyama and the rejections under 35 U.S.C. § 103(a) should be withdrawn.

Dependent Claims 2-11, 13, 14, 16 and 18-21

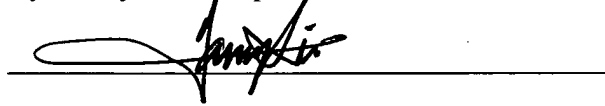
Claims 2-11, 13, 14, 16 and 18-21 depend from independent claims 1, 12, 15 and 17, adding structural features that more particularly define the invention and further distinguish over the cited references and the prior art of record. For these reasons, and for the reasons set forth above for claims 1, 12, 15 and 17, the rejections of these dependent claims under 35 U.S.C. § 103(a) are improper and should be withdrawn.

Conclusion

In view of the above amendments and remarks, it is respectfully submitted that all the pending claims are in condition for allowance, and such action is earnestly solicited. If the Examiner believes that a telephone interview will help further the prosecution of this case, he is respectfully requested to contact the undersigned attorney at the listed telephone number.

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on January 25, 2006.

By: Tanya Kiatkulpiboone



Signature

Dated: January 25, 2006

Very truly yours,

SNELL & WILMER L.L.P.



Ketan S. Vakil
Registration No. 43,215
600 Anton Boulevard, Suite 1400
Costa Mesa, CA 92626-7689
Phone: 714-427-7405
Fax: 714-427-7799